PETER DUKES, University of Victoria
Randomness expansion using orthogonal arrays

Loosely, a pseudo-random number generator (PRNG) turns some short 'random' sequence into a longer sequence which simulates random behavior in some way.

In earlier work, Gopalakrishnan and Stinson demonstrate how a strength two, index one orthogonal array acts as a PRNG. A random row is chosen, requiring two random inputs, and other elements in that row are output as pseudo-random. Although extremely basic by today's standards of PRNGs, some simple and elegant independence bounds exist.

Based on my work with Alan C.H. Ling, this talk explores an extension to higher strength orthogonal arrays. Significantly stronger independence results are possible at the expense of generating a few more initial random inputs.